

Fig. 1

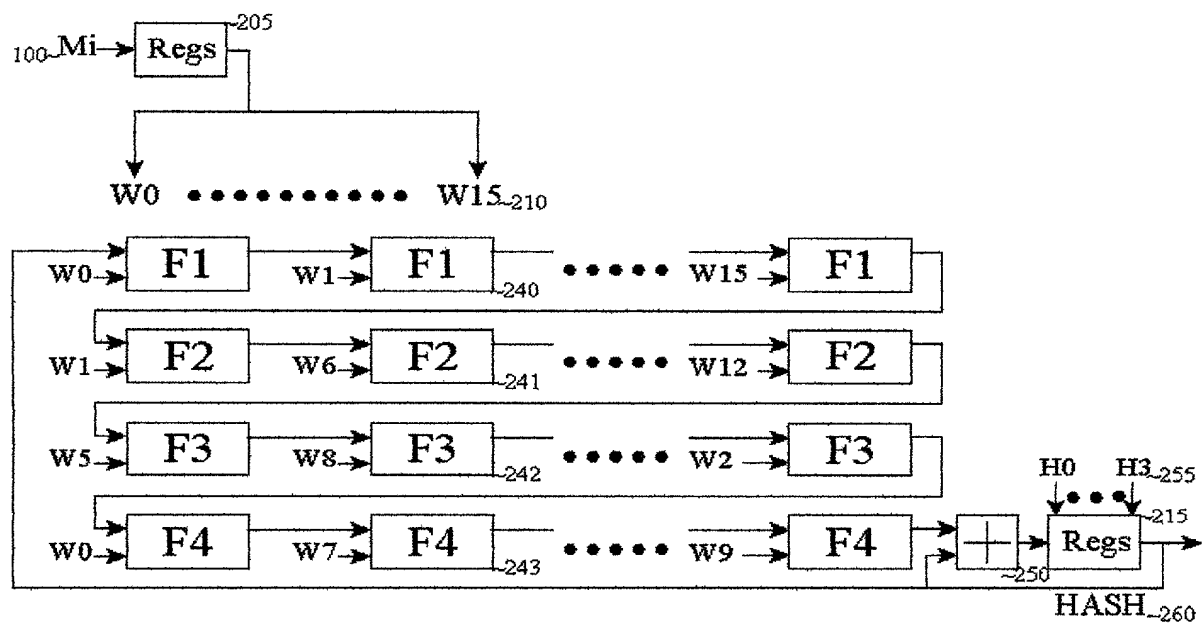


Fig. 2

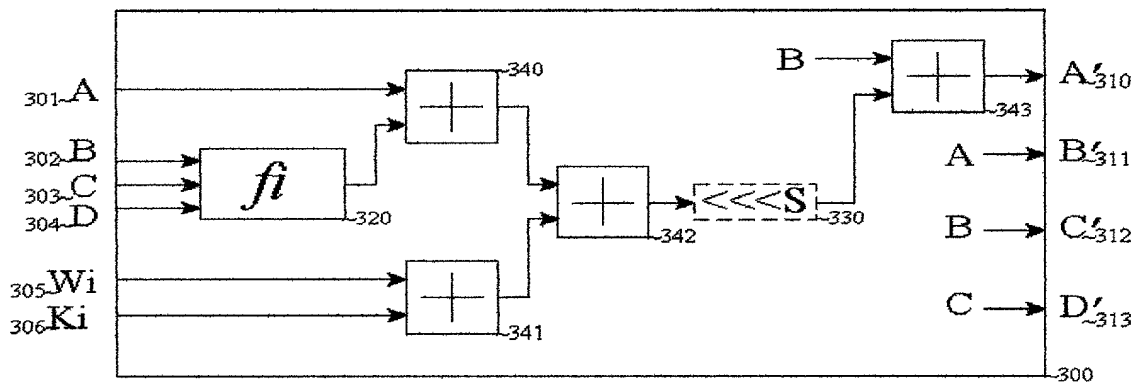


Fig. 3

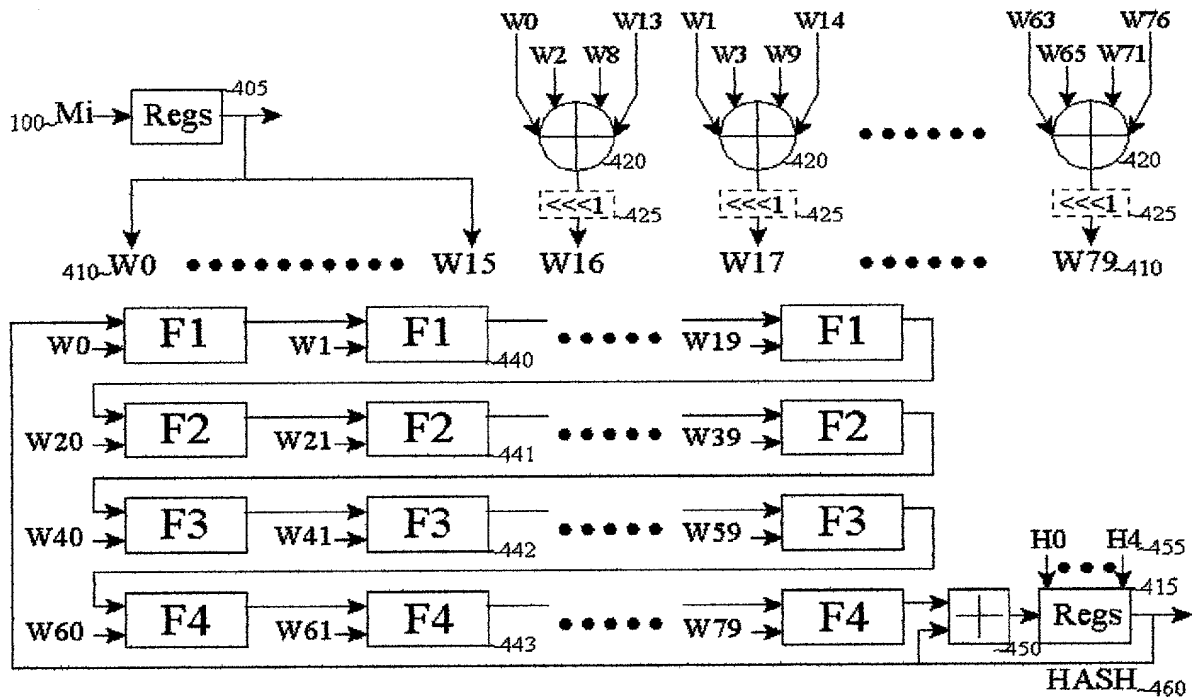


Fig. 4

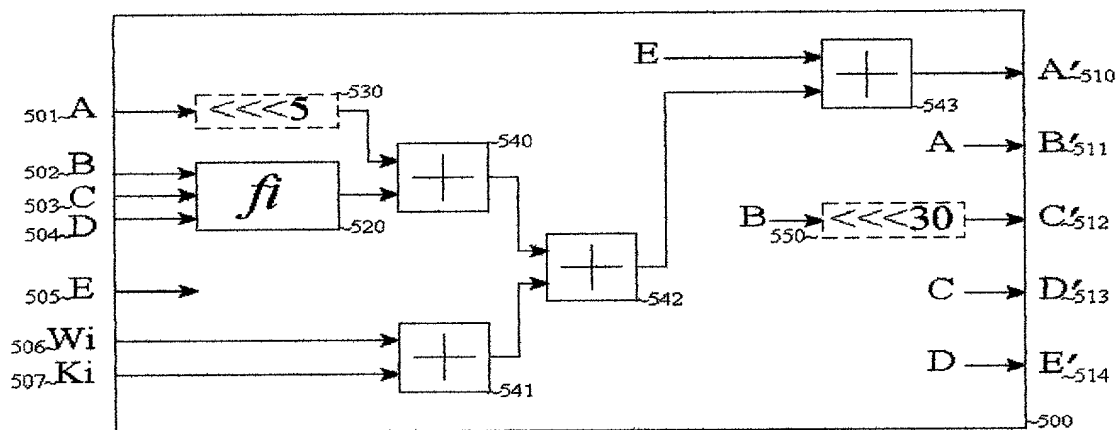


Fig. 5

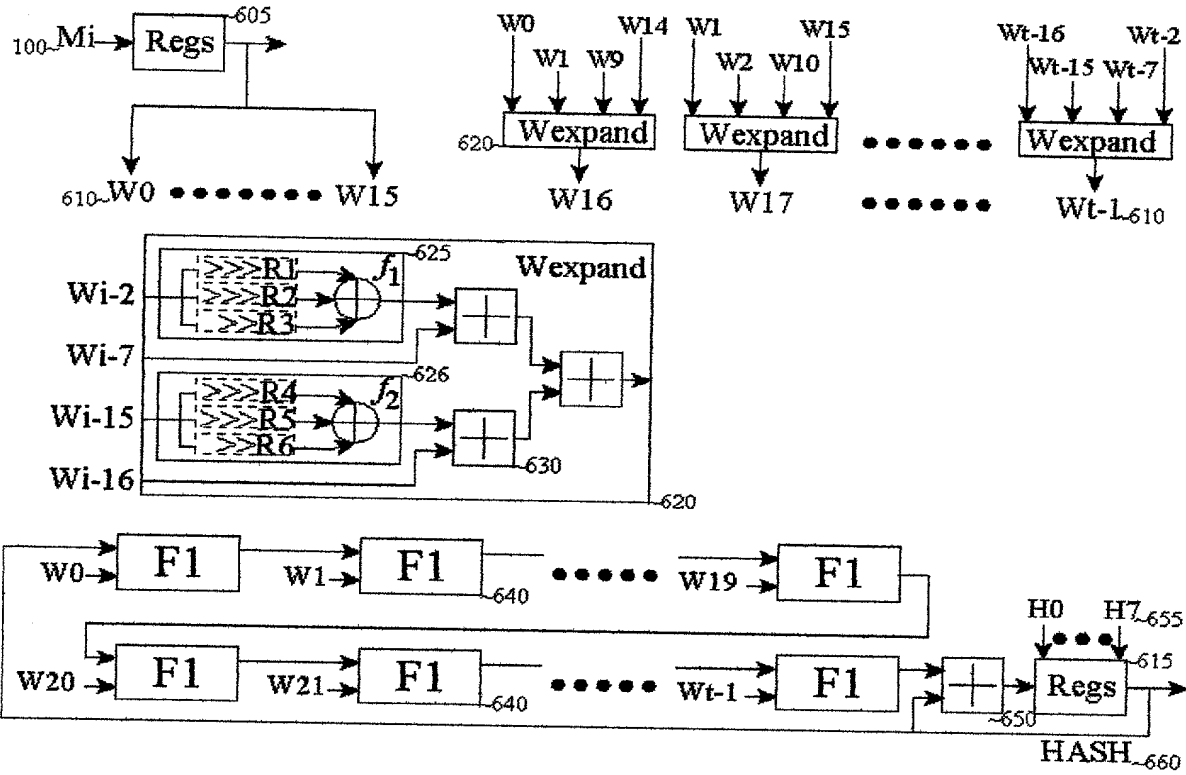


Fig. 6

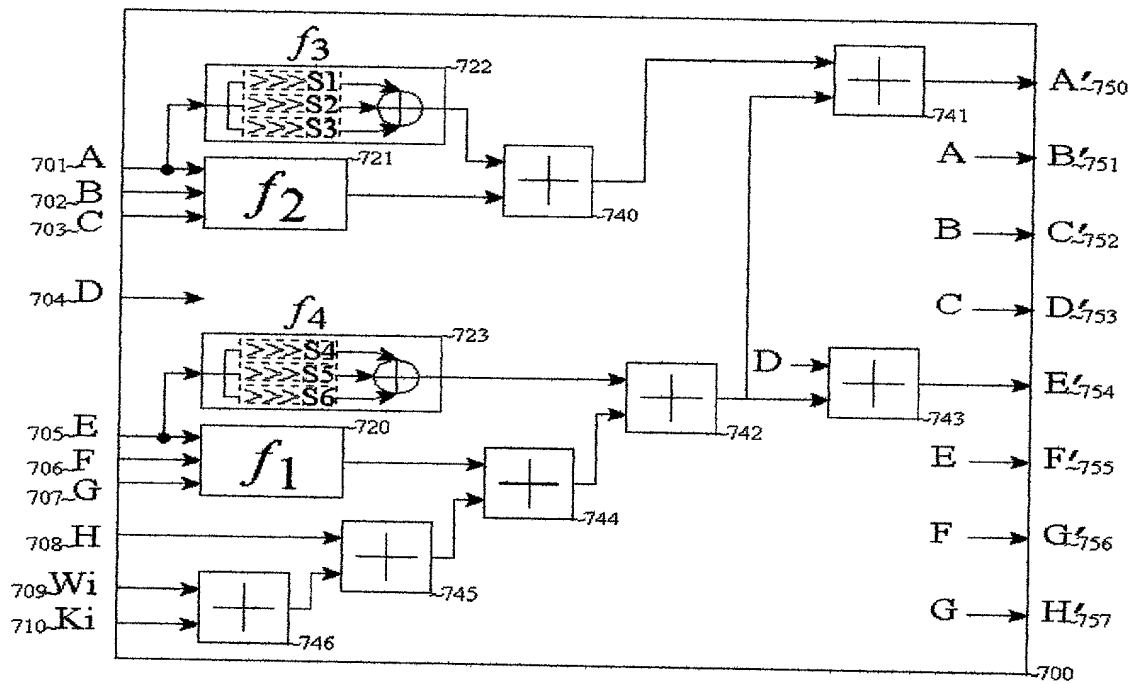


Fig. 7

$$h1(X, Y, Z) = (X \text{ AND } Y) \text{ OR } (\sim X \text{ AND } Z)$$

$$h2(X, Y, Z) = X \text{ XOR } Y \text{ XOR } Z$$

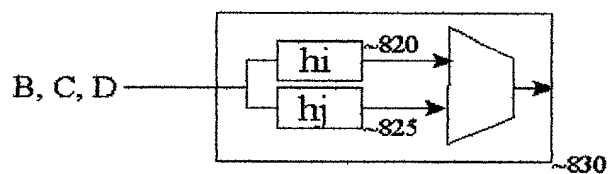
$$h3(X, Y, Z) = (X \text{ AND } Y) \text{ OR } (X \text{ AND } Z) \text{ OR } (Y \text{ AND } Z)$$

$$h4(X, Y, Z) = Y \text{ XOR } (\sim Z \text{ AND } X)$$

(a)

Group	1	2	3	4	5	6	7	8
Rounds	1-16	17-20	21-32	33-40	41-48	49-60	61-64	65-80
MD5	h1	h1'	h1'	h2	h2	h4	h4	
SHA-1	h1	h1	h2	h2	h3	h3	h2	h2

(b)



(c)

Fig. 8

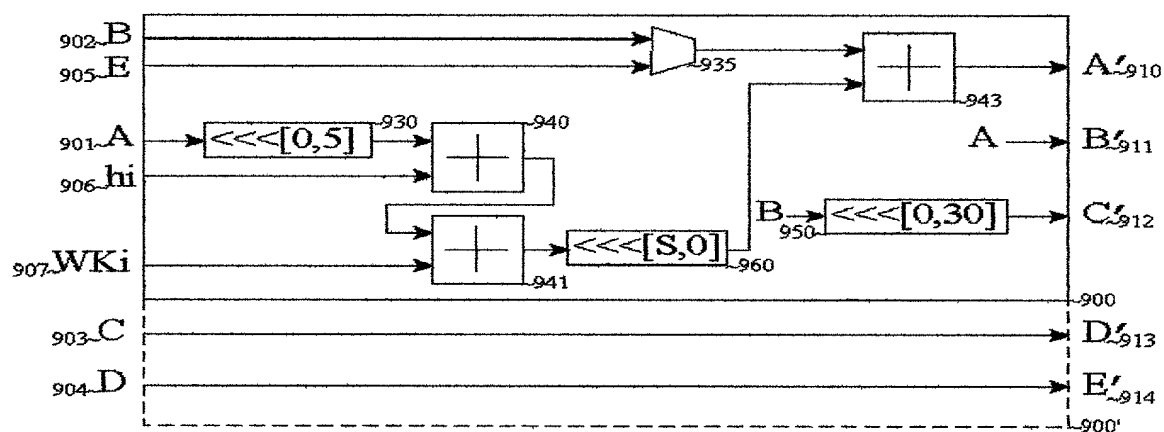


Fig. 9

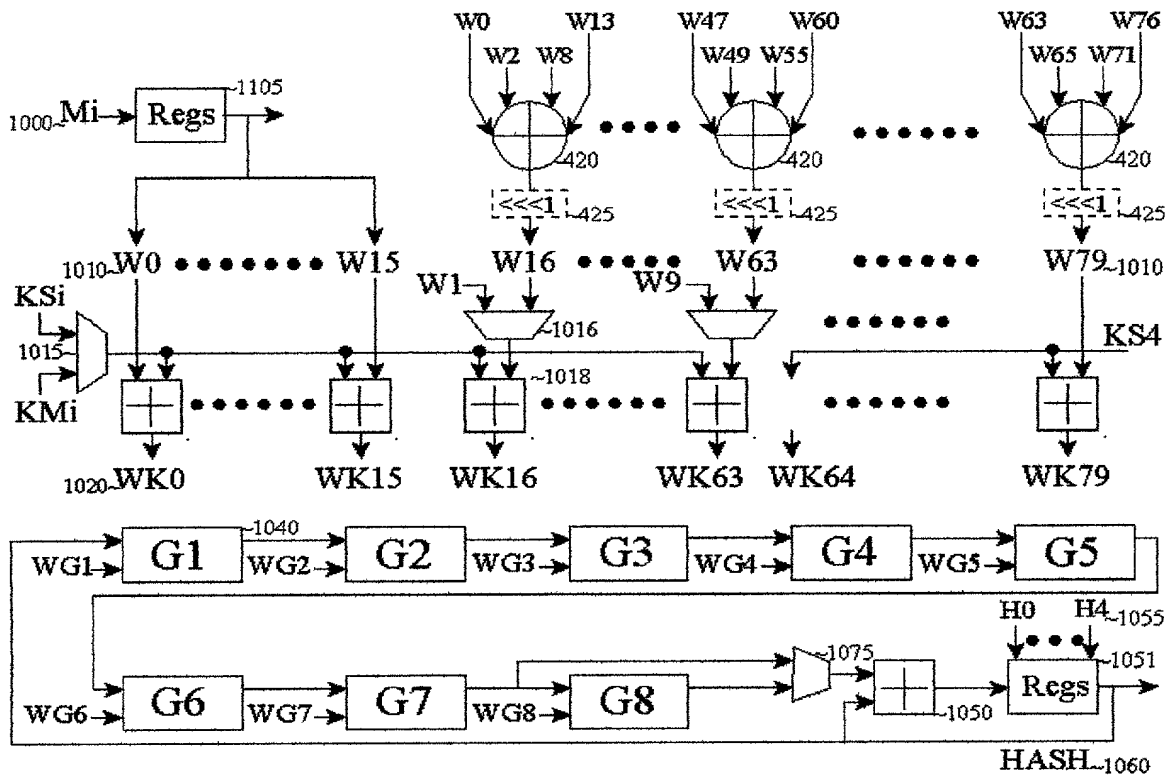


Fig. 10